UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/923,574	08/07/2001	Ronald O'Neal Edmark	AUS920010185US1	2691

35525 7590 08/22/2005

IBM CORP (YA)
C/O YEE & ASSOCIATES PC
P.O. BOX 802333
DALLAS, TX 75380

EXAMINER	
NGUYEN, MINH DIEU T	
ART UNIT	**PAPER NUMBER**
2137	

DATE MAILED: 08/22/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	09/923,574	EDMARK ET AL.	
	Examiner	Art Unit	
	Minh Dieu Nguyen	2137	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *08 June 2005*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-20* is/are pending in the application.

4a) Of the above claim(s) *21 and 22* is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-20* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

Response to Amendment

1. This action is in response to the communication dated June 8, 2005 with the amendments to claims 1-20 and the cancellation of claims 21-22.

2. Claims 1-20 are pending.

3. The amendments to claims 1 and 4-5 have overcome the claim objections and the amendments to the specification are considered.

Response to Arguments

4. Applicant's arguments filed June 8, 2005 have been fully considered but they are moot in view of the new ground(s) of rejection. Applicant's arguments focus on the combination of features introduced by the amendment with elements that already existed in the claims. The new material is rendered obvious by Coley et al. (5,826,014) Rowland (6,405,318) and Bernhard et al. (6,275,942).

5. Applicant argues that Coley does not teach the specific testing step as recited in amended claim 1.

Applicant's arguments are moot in view of the new ground(s) of rejection.

6. Applicant argues that an access request with an "IP spoofing" address as taught in Coley is distinguishable from a request for access to a particular resource.

Examiner disagrees, Coley discloses in col. 10, lines 53-55 that if any incoming access request has a source address of a network element behind the firewall (Fig. 3,

elements 320, 322, 324, 326), (i.e. incoming request includes the source address, i.e. particular IP address to access to a particular piece of information at that IP address) that packet will be intercepted and discarded.

7. Applicant's argues that Rowland does not cure the deficiencies of Coley; that Rowland monitors user logins, not monitors a particular IP address as claimed; that Rowland monitor user login time of day, not monitors the number of requests over a specific quantity of time for a particular IP address as claimed.

Examiner disagrees.

First, Coley discloses the indicia includes a particular IP address (i.e. destination address) in a particular amount of time (col. 9, line 61 to col. 10, line 2). However Coley does not disclose the concept of "context of prior requests".

Rowland discloses a computer-implemented intrusion detection system and method. The system detects unauthorized users attempting to enter into a computer system by comparing user behavior to a user profile wherein the user profiles are dynamically constructed for all user first attempts to log into the computer system and subsequent logins (Abstract), it anticipates context of prior requests. Rowland discloses user profiles are automatically built of the days, times and length of time that the user has logged in (col. 5, lines 21-23) and the odd login time module monitors user logins and attempts (i.e. number of requests for information) to spot "unusual" login times (i.e. any particular time or length of time not recorded in user profiles, col. 9, lines 32-36) based on past data collected for user (i.e. context of prior requests) (col. 9, lines 20-51).

Rowland does not just monitor user logins, the system administrator may select (col. 8, lines 25-31) the log auditing function (Fig. 2) monitors system log files for anomalous activity, the login anomaly detection (Fig. 3) monitors system login and logout audit files, the logout anomaly detection (Fig. 5A/B) monitors something has occurred during the user's login time that may indicate a system anomaly, the session monitor (Fig. 7) monitors user activity for a threat to the computer system and port scan detector (Fig. 6) detects attackers using port scanning method to gain entry to the system.

Claim Rejections - 35 USC § 112

8. Claim 5 is rejected under 35 U.S.C. 112, first paragraph, as failing to comply with the written description requirement. The claim(s) contains subject matter which was not described in the specification in such a way as to reasonably convey to one skilled in the relevant art that the inventor(s), at the time the application was filed, had possession of the claimed invention. The phrase "a predetermined" is not properly described in the application as filed.

Specification

9. The specification is objected to as failing to provide proper antecedent basis for the claimed subject matter. See 37 CFR 1.75(d)(1) and MPEP § 608.01(o). Correction of the following is required: the specifications are not clear on how "a predetermined" is defined.

Claim Rejections - 35 USC § 103

10. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

11. Claims 1-4, 6-17 and 19-20 are rejected under 35 U.S.C. 103(a) as being unpatentable over Coley et al. (5,826,014) in view of Rowland (6,405,318).

a) As to claims 1, 9 and 13, Coley discloses firewall system (i.e. server system) for protecting network elements connected to a public network comprising one or more source servers that store information (Fig. 2, elements 216, 218); a first server (Fig. 2, element 210), communicatively coupled to the one or more source servers and to the network; that receives the incoming request from the network (col. 7, lines 16-18) and the first server testing the incoming request (col. 7, lines 35-39) for an indicia (col. 6, lines 34-39; col. 8, lines 6-9) contained within the request that the request is not valid for the one or more source servers to respond to the request (col. 7, lines 56-57), and passing the incoming request to the one or more source servers when the incoming request is valid (col. 9, lines 13-18).

Coley discloses the indicia includes a particular IP address (i.e. destination address) in a particular amount of time (col. 9, line 61 to col. 10, line 2). However Coley does not disclose the concept of "context of prior requests".

Rowland discloses a computer-implemented intrusion detection system and method. The system detects unauthorized users attempting to enter into a computer system by comparing user behavior to a user profile wherein the user profiles are dynamically constructed for all user first attempts to log into the computer system and subsequent logins (Abstract), it anticipates context of prior requests. Rowland discloses user profiles are automatically built of the days, times and length of time that the user has logged in (col. 5, lines 21-23) and the odd login time module monitors user logins and attempts (i.e. number of requests for information) to spot "unusual" login times (i.e. any particular time or length of time not recorded in user profiles, col. 9, lines 32-36) based on past data collected for user (i.e. context of prior requests) (col. 9, lines 20-51).

It would have been obvious to one of ordinary skill in the art at the time of the invention of employ the use of having a particular IP address in a context of prior requests and the context of prior requests is based on a number of requests for information in the system of Coley as Rowland teaches so as to provide a more rigorous way to detect intrusions for a computer system.

b) As to claims 2, 6, 11 and 15, Coley discloses the one or more source servers transmitting information to the first server in response to the incoming request and the first server re-transmitting the information to the user (col. 12, lines 7-19).

c) As to claims 3 and 7, Coley discloses the first server does not pass the incoming request to the one or more source servers when the incoming request contains indicia that the request is not valid for the one or more source servers to respond to the request (Figs. 4A/B).

d) As to claims 4, 8, 12 and 16, Coley discloses the incoming request is determined to be not valid when the request is for access to a particular resource (i.e. the incoming request specifies a particular network element (particular resource) is intercepted and discarded, col. 10, lines 53-55).

f) As to claims 10 and 14, Coley discloses the step of determining is performed by a software resident on the computing system (col. 13, lines 46-56).

g) As to claim 17, Coley discloses firewall system (i.e. server system) for protecting network elements connected to a public network comprising one or more source servers that store the information (Fig. 2, elements 216, 218); a first server (Fig. 2, element 210), communicatively coupled to the one or more source servers and to the network, that receives the incoming request from the network (col. 7, lines 16-18), the first server detecting an intrusion by the incoming request (col. 7, lines 54-55; line 64 to col.. 8, line 16) based on indicia (col. 6, lines 34-39; col. 8, lines 6-9) of the incoming request being improper, and the first server passing the incoming request to the one or more source servers when the indicia associated with the incoming request indicates that the incoming request is proper (col. 9, lines 13-18).

Coley discloses the indicia includes a particular IP address (i.e. destination address) in a particular amount of time (col. 9, line 61 to col. 10, line 2). However Coley does not disclose the concept of "context of prior requests".

Rowland discloses a computer-implemented intrusion detection system and method. The system detects unauthorized users attempting to enter into a computer system by comparing user behavior to a user profile wherein the user profiles are

dynamically constructed for all user first attempts to log into the computer system and subsequent logins (Abstract), it anticipates context of prior requests. Rowland discloses user profiles are automatically built of the days, times and length of time that the user has logged in (col. 5, lines 21-23) and the odd login time module monitors user logins and attempts (i.e. number of requests for information) to spot "unusual" login times (i.e. any particular time or length of time not recorded in user profiles, col. 9, lines 32-36) based on past data collected for user (i.e. context of prior requests) (col. 9, lines 20-51).

It would have been obvious to one of ordinary skill in the art at the time of the invention of employ the use of having a particular IP address in a context of prior requests and the context of prior requests is based on a number of requests for information in the system of Coley as Rowland teaches so as to provide a more rigorous way to detect intrusions for a computer system.

h) As to claim 19, Rowland discloses the context of prior requests comprises requests for different information from a common computing device coupled over the network (col. 6, lines 36-49).

i) As to claim 20, Rowland discloses the context of prior requests is based on a number of requests for the same information (col. 5, lines 10-15).

12. Claim 5 is rejected under 35 U.S.C. 103(a) as being unpatentable over Coley et al. (5,826,014).

Coley discloses a computing system that preprocesses and monitors incoming requests for information from a user over a network (Fig. 2), the information stored on

one or more source servers communicatively coupled to the computing system (Fig. 2, elements 216, 218), the computing system comprising a network input port that receives the incoming request (Fig. 2, element 206); a source server port (Fig. 2, element 210), communicatively coupled to the one or more source servers, that transmits the information to and from the one or more source servers; an intrusion detection mechanism communicatively coupled to the network input port (col. 7, lines 35-37); the intrusion detection mechanism receiving the incoming request from the network and checking the incoming request for indicia of an invalid request from information associated with the incoming request (col. 7, line 64 to col. 8, line 16); the intrusion detection mechanism transmitting the incoming request to the one or more servers when the indicia associated with the incoming requests are valid (col. 9, lines 13-18).

Coley further discloses the indicia includes a particular IP address in the incoming request (i.e. destination address) in the incoming request in a particular amount of time (col. 9, line 61 to col. 10, line 2). Coley also discloses a large numbers of access requests sending by hackers to inundate a port (col. 4, lines 10-13), the type of very well known attack, a "denial of service attack" anticipates incoming request including a maximum number of requests.

It would have been obvious to one of ordinary skill in the art at the time of the invention to implement incoming request includes a predetermined maximum number of requests by a particular IP address in a particular amount of time in the system of Coley as invalid indicia so as to provide a more rigorous way to detect intrusions for a computer system.

13. Claim 18 is rejected under 35 U.S.C. 103(a) as being unpatentable over Coley et al. (5,826,014) in view of Rowland (6,405,318) and further in view of Bernhard et al. (6,275,942).

Rowland discloses the context of prior requests, however he does not disclose the context of prior requests comprises requests for the same information.

Bernhard discloses a system, method and computer program product for automatic response to computer system misuse comprising the context of prior requests comprises requests for the same information (col. 1, lines 63-67).

It would have been obvious to one of ordinary skill in the art at the time of the invention to employ the use of comprising requests for the same information in the context of prior requests in the system of Coley and Rowland, as Bernhard teaches so as to effectively detect intrusions as they occur.

Conclusion

14. Applicant's amendment necessitated the new ground(s) of rejection presented in this Office action. Accordingly, **THIS ACTION IS MADE FINAL**. See MPEP § 706.07(a). Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not

mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the date of this final action.

15. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Minh Dieu Nguyen whose telephone number is 571-272-3873. The examiner can normally be reached on M-F 6:00-2:30.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Emmanuel Moise can be reached on 571-272-3865. The fax phone number for the organization where this application or proceeding is assigned is (703) 872-9306.

Any inquiry of a general nature or relating to the status of this application or proceeding should be directed to the receptionist whose telephone number is 571-272-2100.

Minh Dieu Nguyen
Examiner
Art Unit 2137

mdn
8/9/05

EMMANUEL L. MOISE
SUPERVISORY PATENT EXAMINER